Lobachevskii Journal of Mathematics 2013 vol.34 N4, pages 313-315

Using frequency analysis and Grover's algorithm to implement known ciphertext attack on symmetric ciphers

Ziatdinov M.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

In this paper we construct quantum circuit implementing known ciphertext attack on symmetric cipher. We assume that plaintext is in natural language and have known letter distribution. Our method allows to find key using one query to (quantum) decryption oracle and has O(√{pipe}K{pipe}) time complexity, where K-set of possible keys. © 2013 Pleiades Publishing, Ltd.

http://dx.doi.org/10.1134/S1995080213040148

Keywords

frequency analysis, Grover's algorithm, known ciphertext attack, quantum fingerprinting, symmetric ciphers